MAIN THREATS TO CLOUD COMPUTING SECURITY

Ms. Keren Daniel
Assistant Professor
St. Xaviers College, Jaipur

Abstract

CLOUD COMPUTING – Cloud computing has been significantly bringing changes to parallel computing and distributed computing in the current trend. It is an on- demand computing to the IT industry. Cloud computing provides the user a high quality of feasible solution as compared with other infrastructures. It gives full scalability, flexibility, efficiency and reliability on the accessed hardware/software infrastructure in the internet. It gives services without upfront investment in IT services. Security has been the issue that is constantly talked about for networking and internet. Cloud computing comprises of several virtual machine running on same platform which is seen physical attacked by threats. The paper we discuss the complexities of different threats to cloud computing. If security issues are not addressed the creditability of Cloud Computing will decrease.

Keywords: Cloud Computing, VMs, Security Issues

Introduction

Cloud computing means an "Internet computing" where collection of clouds is seen on the internet. It is a network-based environment that helps in sharing computations or resources to others. It provides references to both the applications delivered on the Internet. Virtualization technologies are used in cloud computing which combines with self-service abilities for computing resources through network infrastructure. In cloud, several kinds of virtual machines are hosted on the same physical server as infrastructure. In cloud, costumers pay for the resources used and not for the resources not accessed.

Cloud computing is an independent when compared with other utility computing. Eg Google Apps is an apt application where cloud computing is used, where millions of computers are brought into effective action and functioning in the internet. There are three types of cloud computing Public, private and hybrid. Resources are cheaper when compared with other computing resources. Cloud is accessible throughout the globe anytime. Cloud computing can also be defined as it is a new service, which are the collection of technologies and a means of supporting the use of large scale Internet services for the remote applications with good quality

of service (QoS) levels [4].

The attributes of cloud computing are

- Automation of administrative tasks.
- Scalability
- Elasticity
- Access to internet anytime

Model Of Cloud Computing

Cloud computing has two main models that help in delivery of information using the technologies.

1. **Service model -**In this model the computing technologies that are considered are Saas ("Software as a Service"), Paas ("Platform as a Service"), IaaS (Infrastructure as a Service"). The types of services have been explained below.

A. **Infrastructure as a service model,** enables the virtul and physical hardware as service and the full infrastructure is given on the internet. It provides networking, virtualization, servers and storage[5].

B. **Platform as Service Models,** gives a base for development and deployment of software applications. It also provides runtime, middleware, OS, networking, servers. The Operating system's features can be changed using this service [6]. This models also offers the customers greater controllability and extensibility.

C. **Software as a Service model,** in this model the security, management and control are administered by the provider. The characteristics of SaaS are:

- Human resource management
- Making invoice
- Collaboration
- Managing the document

2. **Delivery models**

A. **Private cloud**: The proprietor does not give away with the resources with any other organizations. In this security can be well executed.[8,9].

B. **Public cloud:** in this model it based on “pay on basis” which is billed by the provider.

C. **Hybrid cloud:** It is mainly made for the business world based on customer's requirement. Private cloud is linked with external cloud.

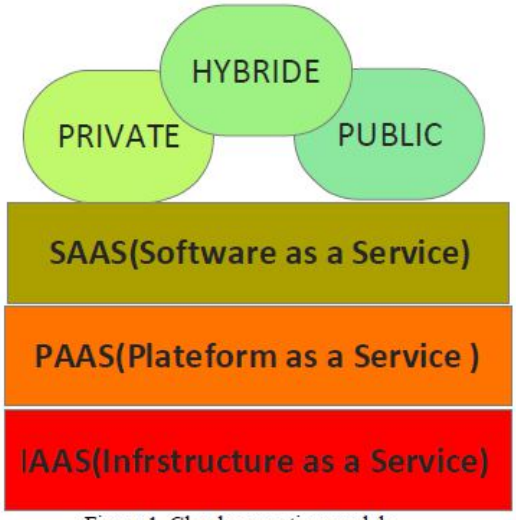

Figure 1. Cloud computing models

Security Issues in Cloud Computing

In cloud computing recently there are nine threats have been studied which are explained below:

A. **Data Breaches**

This results in loss of personal information and card details of many indivuals. Breaches occur through hypervisors and virtual machines eventually as cloud computing is on networking. A data breach is the result of a malicious and probably intrusive action.

B. Data Loss

Data loss may occur when a disk drive dies without its owner having created a backup. It occurs when the owner of encrypted data loses the key that unlocks it. And a data loss could occur intentionally in the event of a malicious attack. "For both consumers and businesses, the prospect of permanently losing one's data is terrifying.

C. Account or Service traffic hijacking

Phishing, exploitation of software vulnerabilities such as buffer overflow attacks, and loss of passwords and credentials can all lead to the loss of control over a user account. An intruder with control over a user account can eavesdrop on transactions, manipulate data, provide false and business-damaging responses to customers, and redirect customers to a competitor's site or inappropriate sites.

D. Insecure APIs

API that defines how a third party connects an application to the service and providing verification that the third party producing the application is who he says he is. Implementation of Auth-supporting APIs by third party developers can be flawed as well."From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

E. Denial of service

Denial of service attacks is an old disrupter of online operations, but they remain a threat nevertheless. For cloud customers, "experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock:

F. Malicious insiders

"If the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack." Systems that depend "solely on the cloud service provider for security are at great risk" from a malicious insider.

G. Abuse of cloud services

Cloud computing brings large-scale, elastic services to enterprise users and hackers alike. "It might take attacker years to crack an encryption key using his own limited hardware. But using an array of cloud servers, he might be able to crack it in minutes.

H. Insufficient of due diligence

"Too many enterprises jump into the cloud without understanding the full scope of the undertaking. Without an understanding of the service providers' environment and protections, customers don't know what to expect in the way of incident response, encryption use, and security monitoring. Not knowing these factors means "organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks.

I. Shared technology

The cloud is about shared infrastructure, and a misconfigured operating system or application can lead to compromises beyond their immediate surroundings.

Conclusion

Cloud computing provides lots of advantages but today, cloud computing is suffering from security. Security is a biggest concern of client these days. If client want to take full advantage of cloud computing so client must

ensure about data, infrastructure and application security. In this paper we provide a different threats for cloud which causes the organizational physical and virtual assets to downfall.

WORKS CITED

1. "Cloud Computing:security Model Comprising Governance, Risk Managemnt and Compliance", Fawaz S AL-Anzi, Sumit Kr Yadhav, Jyoti Soni,Computer Engineering Department, Kuwait University.
2. Dr. L.S.S.REDDY, International Journal of Engineering Science and
3. Technology (!JEST), Vol. 3 No. 9 September 2011.
4. http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085?page_number=1
5. Chopde, International lournal of Computer Applications (0975 - 8887) Volume 34- No.9, November 2011
6. "Cloud Computing Security" Danish Jamil Hassan Zaki, Internationallournal of Engineering Science and Technology (IJEST), Vol. 3 No. 4April 201 I
7. http://www.cloudsecurityalliance.org
8. Kitchenham B (2004) Procedures for perfoming systematic review, software engineering group. Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd, Australia. TR/SE-0401
9. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering. Version 2.3University of keele (software engineering group, school of computer science and mathematics) and Durham. Department of Conputer Science, UK
10. Pappas, Vasilis, et al. "CloudFence: Data Flow Tracking as a Cloud Service."Research in Attacks, Intrusions, and Defenses. Springer Berlin Heidelberg, 2013. 411-431.
11. Seccombe, A., et al. "Security guidance for critical areas of focus in cloud computing, v2. 1." Cloud Security Alliance (2009).